PART 2

Emerging Trends
Digital Public Infrastructure: Transforming Service Delivery Across Sectors
Jonathan Marskell, Georgina Marin, and Minita Varghese

KEY MESSAGES

• Digital public infrastructure (DPI) is a new term referring to the basic capabilities that are building blocks for developing digital services at a societal scale. DPI is the intermediate layer between physical infrastructure (for example, broadband and data centers) and sectoral applications (for example, social protection and e-commerce). The most common types of DPI are platforms and systems for digital identification (ID), digital payments, and data sharing.

• DPI rose in prominence during the COVID-19 pandemic. The countries that had elements of DPI in place before the pandemic were generally more resilient. Research by the World Bank’s Digitalizing Government-to-Person Payments initiative has found that these countries reached three times more beneficiaries with emergency cash transfers. Countries with good DPI in place could also keep government services, commerce, hospitals, schools, and other operations functioning through online channels.

• Globally, 850 million people lacked any form of official ID in 2021. Five billion people live in countries without a digital ID that can be used for secure online access to public and private sector services.

• Only 96 economies have fully operationalized both the legal frameworks and the technological infrastructure (for example, public key infrastructure) for e-signatures, which are a key source of trust in the digital economy. Two-thirds are high-income and upper-middle-income economies. Likewise, only 89 economies have a functional data exchange platform, with three-quarters being high-income and upper-middle-income economies.

• While the percentage of adults with a formal financial account in low- and middle-income countries jumped to 71 percent in 2021 (from 63 percent in 2017), only 57 percent of adults made or received some sort of digital payment and only 37 percent made one with a merchant. One significant opportunity is the rapid rise in fast or real-time payment systems, which have been launched or announced in about 100 jurisdictions.

Introduction
With a few taps on their mobile phone, remote area workers in India can apply for social benefits to be paid directly into their bank account and electronically sign an application for a loan. In Thailand, farmers can receive fertilizer subsidies into a bank account linked to their identification (ID).
In Singapore citizens and residents can conduct almost any transaction end-to-end online, no matter where they are, from registering a birth to filing taxes and opening a new business. These services are made possible through innovations catalyzed by digital public infrastructure.

This chapter introduces a new concept—digital public infrastructure (DPI)—and illustrates its growing significance to all aspects of the digital economy. The chapter also summarizes different models for developing certain DPI elements, notably ID and data exchange platforms. The chapter then identifies some key gaps in developing countries’ DPI systems, and highlights general principles, risks, and challenges when developing DPI systems.

**What is DPI, and why is it important?**

DPI refers to the basic capabilities—such as for identification, payments, and data sharing—that are the building blocks for developing transformative digital services at a societal scale. At its simplest, DPI can be understood as an intermediate layer in the digital ecosystem (refer to figure 4.1). It sits atop a physical layer (including internet connectivity, devices, servers, data centers, the cloud, and routers) and enables applications across various sectors (for example, information systems and solutions to different verticals, e-commerce, social protection, remote education, and telehealth). The focus on reusable and horizontal foundations is a paradigm shift from conventional approaches to digitalization that have, in many cases, led to fragmentation and siloes. Some examples of DPI include India’s Aadhaar identification system, Brazil’s Pix fast payment system, and Australia’s Consumer Data Right for consented sharing of personal data. Since reliable verification and the flow of money and information are at the core of most digital transactions, DPI prevents the need for the owner of an application to reinvent the wheel (Desai et al. 2023). Furthermore, when open and interoperable, DPI can promote innovation, competition, productivity gains, and other democratizing and multiplier effects at the application layer and across sectors (Global Partnership for Financial Inclusion 2023).

Awareness about the importance of DPI grew during the COVID-19 pandemic. As described later in this chapter, the countries that had elements of DPI in place before the pandemic were able to mount social protection responses more quickly, transparently, and effectively. For example, Thailand benefited from the ability of people to link their digital ID to a bank or e-wallet account.

**FIGURE 4.1 The concept of digital public infrastructure**

(a) Conventional approaches to digitalization

(b) New approach to digitalization

Note: ID = identification.
When a new program for informal workers had to be rolled out quickly via online registration, this ability provided greater assurance that the right person was receiving emergency cash transfers. Countries with DPI were also better equipped to adapt as businesses, government agencies, schools, and hospitals shifted to digital and online channels.

However, while the term is new, the concept of DPI traces its roots to the earlier experience of advanced digital countries. Even before the pandemic, some of the fastest-growing digital economies and most dynamic digital governments—including Brazil, Estonia, Kenya, and the Republic of Korea—built much of their success in making lives easier and creating economic opportunities on cross-cutting platforms for identifying people and businesses (and related trust services such as e-signatures, consent, verifiable credentials, and data vaults), interoperable fast payments, and seamless and secure data sharing. Countries are also beginning to apply DPI to climate change mitigation and adaptation, such as to optimize energy generation using peer-to-peer energy trading. India’s India Stack (refer to figure 4.2) and Singapore’s Digital Utilities are examples of how countries have layered the elements of DPI with interoperability enabled by application programming interfaces (APIs), making the whole greater than the sum of the parts and creating opportunities for new products and services. The term DPI emerged in late 2021 (Rockefeller Foundation, Digital Public Goods Alliance, and Norway Ministry of Foreign Affairs 2021) and early 2022 (Metz et al. 2022).

In August 2023, the G-20 reached the first multilateral consensus on a description of DPI and suggestive guiding principles (refer to figure 4.3). This agreement was negotiated among the G-20 digital economy ministers, spearheaded by the Indian Presidency’s Initiative and endorsed by the G-20 leaders. It lays a framework for a common understanding and future international cooperation. Notably, the G-20 outcome recognizes digital ID, digital payments, and data sharing as basic DPI, while also acknowledging that countries will have their own ways and architectures of implementing them. Furthermore, it recognizes that countries may have other forms of DPI to meet the same objectives of underpinning digital service delivery across sectors (refer to box 4.1). For example, India considers its Open Network for Digital Commerce, which is an open communication protocol that connects buyers and sellers across different platforms (from e-commerce to gig work), to be a DPI. Furthermore, the Global Partnership for Financial Inclusion has developed policy recommendations on how DPI can promote financial inclusion and productivity gains. Building on this global momentum, the World Bank has incorporated DPI in one of its five new global priority programs (on accelerating digitalization), and the United Nations has launched a high-impact initiative on DPI to spur progress across all 17 United Nations Sustainable Development Goals (SDGs).

The “public” in DPI refers to public benefit and common good, not government ownership. The intention is to convey that digital ID, digital payments, data sharing, and other foundational capabilities are just as important for the functioning and transformation of economies and societies in today’s digital age as physical infrastructure like roads and railways were in previous centuries,
FIGURE 4.3 G-20 DPI outcomes in 2023

G20 description of DPI:
Under the Indian Presidency’s initiative, we recognize that digital public infrastructure, hereinafter referred to as DPI, is described as a set of shared digital systems that should be secure and interoperable, and can be built on open standards and specifications to deliver and provide equitable access to public and/or private services at societal scale and are governed by applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms. Considering the diverse approaches of G20 members to digital transformation, we recognize that DPI is an evolving concept that may not be limited to sets of digital systems with these characteristics and could be tailored to specific country contexts and can be referred to with different terminologies.

G-20 framework for systems of DPI: Suggested principles:
- Inclusivity
- Interoperability
- Modularity and extensibility
- Scalability
- Security and privacy
- Collaboration
- Governance for public benefit, trust, and transparency
- Grievance regress
- Sustainability
- Human rights
- Intellectual property protection
- Sustainable development

Indicative, voluntary, and nonbinding policy recommendations for advancing financial inclusion and productivity gains through the use of DPIs in the financial sector:
- Enable and foster the use of DPIs to accelerate financial inclusion and productivity gains
- Develop well-designed DPIs and the broader enabling environment through a widely accepted set of good practices
- Encourage appropriate risk-based regulation, supervision, and oversight arrangements for financial sector use of DPIs
- Promote sound internal governance arrangements
- Enable DPIs to offer products and services in a way that no one is left behind and the interests of consumers are safeguarded

BOX 4.1 Different approaches to DPI

The approach to governing and implementing digital public infrastructure (DPI), including individual layers, will differ markedly among countries, reflecting differences in the political economy, legal, and sociocultural circumstances of the country as well as the desired outcomes. Some factors that will be different include the level of private sector involvement, the extent of centralization or coordination of responsibilities in government, and how the different layers of DPI are architected and made interoperable (if at all).

In the case of digital identification, there are three well-established architectural approaches that, importantly, are not necessarily mutually exclusive:

- **Centralized.** A centralized approach has a single authority (typically a government agency) for issuing and authenticating identity credentials. Examples include India’s Aadhaar and Singapore’s Singpass. The advantage of this approach is its simplicity for users and service providers. The disadvantage is the absence of choice for users and service providers, potentially monopolistic effects on pricing, and the possibility of limited incentives for innovation.

- **Federated.** A federated approach has an ecosystem of authentication providers (from the public or private sectors or both) that users can choose from, operating according to common standards to achieve interoperability and portability. Although there are several providers of...
BOX 4.1 Different approaches to DPI (Continued)

identity credentials and authentication services, the data they use are typically from a centralized source, such as a national identification (ID) system or civil registry. Examples include France’s FranceConnect and Thailand’s National Digital ID platform. The advantages of this approach are the provision of choice, incentivization of innovation, and lower pricing through competition. The disadvantages are potential complexity for users and the need for strong supervisory and regulatory capabilities, which are often lacking in low- and middle-income countries.

• **Decentralized.** This emerging approach involves authentication against a credential that is fully controlled by the user (for example, a digital wallet on a smartphone). In contrast to the other two architectures, the issuer of the identification (for example, a national ID or driving license authority) will not know about authentications that take place, since this verification is done against the credential, typically using asymmetric cryptography. To date, there are no known national-scale implementations; however, the approach is proposed as part of the new European digital wallet initiative and was launched in mid-2023 in Bhutan. The advantages are the increased privacy and potential for greater interoperability and portability. The disadvantage is the complexity for users and service providers, especially vis-à-vis the other architectures.

For data sharing, there is not yet a well-established taxonomy. However, different approaches reflect local political and legal contexts. For example, countries with centralized approaches to digital identification are more likely to have centralized approaches to data sharing. Three factors can vary between countries:

• **Level of centralization.** Some countries, like Belgium (Federal Service Bus), Estonia (X-Tee), Singapore (APEX), and Uganda (UGHub), have developed central mechanisms to facilitate data sharing. These central mechanisms take different technological approaches. For example, Singapore’s APEX is simply an application programming interface marketplace for government to facilitate bilateral point-to-point data sharing, whereas Estonia’s X-Tee involves middleware and a central service bus or hub that orchestrates data sharing. Other approaches, such as those taken in Australia and the United Kingdom, are more sectoral, federated, and standards based.

• **Level of user-centricity.** The first dimension is the extent to which consent is required for the sharing of personal data, which will be a function of the applicable personal data protection law. Singapore’s Singpass and Estonia’s Digital ID are examples of how consent is provided. The second dimension is the amount of control that data subjects have over the process of sharing their data. For example, India’s DigiLocker and the United Arab Emirates’ UAE Pass Digital Vault allow data subjects to store and share their digital documents (that is, data) inside their own devices. Emerging standards for verifying credentials, such as by the World Wide Web Consortium, are taking this a step further by following an approach similar to decentralized identity, described above. One of the first implementations of such an approach at a national scale is Cambodia’s Verify.gov.kh system.

• **Approach to cross-border data flows.** There are three broad approaches to cross-border data flows: open transfer (typically regulated by industries and with no mandatory conditions or approvals for data transfers); conditional transfer (with white listing of recipient countries, incorporation of standard contractual clauses, adoption of domestic certification, and consent); and limited transfer (localization requirements and mandatory explicit regulatory approval). These approaches apply not only to personal data, but also to other forms of data that fuel digital and other trade—for example, data flowing from Internet of Things devices in a factory in country B and going to controllers or supervisors at a company’s headquarters in country A.
with nondiscriminatory access in accordance with governance rules. Additionally, Poole, Toohey, and Harris (2014) argue, “‘Public’ infrastructure is an investment where the government has the primary role in, and responsibility for, deciding on whether and how the infrastructure is provided in the interests of the broader community and ... extends beyond infrastructure that is owned or directly funded by the public sector.” This definition can be expanded to cover this new concept of DPI. In fact, the private sector has a key role to play in the design and implementation of DPI—for example, as developers of use cases and services that drive adoption, as service providers and sources of innovation for development of DPI, as operators of DPI, and as participants in public-private partnerships and other collaborations to achieve scale.

As recognized by the G-20, DPI is just as much about governance and community as it is about technology. The paradigm shift toward a horizontal mind-set for digitalization can only be realized if there is a whole-of-country approach that facilitates coordination across government (including regulators) and collaboration with the private sector, civil society, and other stakeholders. The other necessary elements of governance include transparency and accountability, political will to clarify roles and responsibilities, and legal and institutional safeguards to protect against misuse. With many good-practice examples around the world and a growing number of open standards, open-source software, and other digital public goods, technology may be the easiest part of DPI to solve. For example, as of August 2023, 22 countries are using the X-Road open-source software as the platform for exchanging data (Nordic Institute for Interoperability Solutions 2023), and 11 countries are using the Modular Open Source Identity Platform.1

DPI plays a fundamental role in using digital technologies to enhance service delivery in various domains. Box 4.2 summarizes some emerging evidence on the impact of DPI.

---

**BOX 4.2 Growing evidence on the impact of DPI**

Digital public infrastructure (DPI) represents a transformative shift in a country’s approach to digitalization. The broad theory portrayed in figure B4.2.1 can be applied to any element of DPI. Implementation of one or more elements of DPI is expected to act through various mechanisms to improve individual welfare, facilitate public services and efficiency, and enable commerce and innovation. As the adoption of DPI continues to scale up, it may become possible in the future to measure the distinct impact of applying a DPI approach in addition to studying the effects of its specific subcomponents.

**FIGURE B4.2.1 Theory of change**

Note: G2P = government-to-person.

(Continued)
BOX 4.2 Growing evidence on the impact of DPI (Continued)

The examples that follow provide early evidence to support this hypothesis. However, these interventions entail the same risks as any digitalization: exclusion of persons with low digital access, skills, or literacy; misuse or mismanagement of personal data; and system lock-in and waste. It is important for research to attempt to capture both negative and positive consequences of DPI design.

Benefits for people

Digital government-to-person (G2P) payments offer a gateway to financial inclusion and other benefits:

• According to the Global Findex 2021, digitalizing G2P payments has contributed to 865 million people worldwide opening their first financial institution account to receive money from the government (Demirgüç-Kunt et al. 2022).

• Brazil. Pix plus digital wallets with remote onboarding plus pro-digital policies contributed to 75 percent of Auxílio Emergencial cash transfer beneficiaries using the funds digitally (Lara de Arruda et al. 2022).

• Mozambique. Beneficiaries spent less than 30 minutes waiting for mobile money payments versus more than one hour waiting for cash payments (World Bank, forthcoming).

• India. The use of digital payments reduced delays in the payment of maternal health conditional cash transfers by 43 percent.

DPI can empower women by ensuring that they receive and control G2P transfers:

• Pakistan. Digital identification–linked cash transfers increased women’s reported control over cash by 9 percentage points (Clark et al. 2022).

• Niger. Households where women received digital social assistance payments had 16 percent higher diet diversity than those who received benefits in cash (Aker et al. 2016).

• India. Digital payments increased female employment outside the household (Field et al. 2021).

DPI for online services can make lives easier:

• Singapore. eKYC, facilitated by the Singpass consented data-sharing service, reduced the time to complete digital transactions by 80 percent (OECD 2022).

• Estonia. The government, citizens, and residents save 820 years of working time every year thanks to the X-Tee data-sharing platform (Vainsalu 2017).

Benefits for businesses

Digitalization of G2P payments can expand access and improve services:

• Zambia. Choice-based payments under the Girls Education and Women’s Empowerment and Livelihoods project allowed for greater competition among payment service providers, improved customer service (travel time dropped from six to two hours), and lowered transaction fees (cash-out fees dropped from US$3.35 to US$2.34) (Baur-Yazbeck, Hobson, and Chirmba 2021).

DPI can lower the cost of doing business:

• India. The typical firm’s onboarding cost is about Re 1,500 (US$23), which, through increased que- riability, digitization, and interoperability of the Aadhaar system, is estimated to reduce onboarding costs to as little as Re 10 (US$0.15) (World Bank 2018).

(Continued)
Key gaps remain in access to IDs, e-signatures, data exchange, and digital payments

Government-recognized digital identification and authentication (that is, digital ID) for people and businesses are a critical function for digital interactions with governments, businesses, and other service providers—and thus the digital economy more broadly—but they are still not widely available. Their absence presents a significant barrier, as having a secure way to prove identity online is an important gateway for full participation in the digital economy. One estimate has found that digital ID can unlock economic value equivalent to 3–13 percent of gross domestic product (White et al. 2019). More fundamentally, a digital ID to transact securely online, especially through a mobile phone, can help citizens, small merchants, farmers, and poor households in rural and remote areas to access more services, markets, formal employment (for example, some gig work), and other opportunities being created by the digital economy. This equalizing effect is why countries such as Brazil, Indonesia, and Rwanda, for example, have recently launched digital ID initiatives with support from the World Bank. Box 4.3 elaborates on the example of Fayda (Ethiopia), FranceConnect (France), and eFaas (Maldives).
BOX 4.3  Examples of digital IDs: Ethiopia’s Fayda, France’s FranceConnect, and Maldives’ eFaas

Ethiopia’s Fayda

Fayda (meaning “value” or “utility” in several local languages) is Ethiopia’s voluntary foundational digital identification (ID) system. Launched as a pilot in 2022, Fayda is addressing the fragmentation and exclusion caused by the existing IDs issued by local governments (kebeles), which cannot be verified, are not very secure, and cannot provide assurance as to the uniqueness of an individual (for example, to support delivery of social transfers). Fayda intends to be the basis for a broader digital public infrastructure ecosystem, including for consented data sharing and digital payments.

Using the Modular Open Source Identity Platform as the foundation of the system, much of the development and integration with specialized components for biometric recognition and other functions have been done in-house. Apart from the ID card, registered users can also download a digital equivalent of their ID in applications maintained by partners, such as mobile network operators and banks. More than 3 million people have registered with Fayda to date.

France’s FranceConnect

Launched in 2016, FranceConnect is a federated digital ID ecosystem that allows French citizens and residents to access more than 1,500 public services online with their choice of digital ID provider from the public and private sectors. When users access a service through a website or application, they can select a digital ID provider with which they already have an account (for example, the post office or a mobile network operator) to authenticate themselves or create an account, with their identity verified based on data in relevant government registries and the “strength” of the digital ID (low, substantial, and high level) based on which data sources and documents they are using to log in. Some higher-risk public services, such as tax returns, may require a minimum strength of substantial or high.

Interoperability is enabled by following the OpenID Connect open standard, and FranceConnect can be used to access public services anywhere in the European Union since it is part of the Electronic Identification and Trust Services (eIDAS) regulation trust framework. The FranceConnect (Continued)
An estimated 850 million people globally still do not have any official ID, an additional 220 million do not have a digital record of their identity, and an additional 400 million do not have a digitally verifiable identity document or identity records. These gaps are heavily concentrated in groups that may be vulnerable and marginalized, such as women, youth, low-income individuals, those in rural locations or with less education, and people out of the workforce (refer to figure 4.4). Closing this gap is key to achieving SDG target 16.9 to, “by 2030, provide a legal identity for all, including birth registration.”

More than 5 billion people (or 3.5 billion adults) do not have access to systems and credentials that would enable secure, remote digital authentication to facilitate access to online services and transactions. Even in the 75 economies where such digital identity solutions exist for transacting online—mostly in high-income countries—there are gaps in the ease of obtaining and using the required digital credentials, the ease of subsequent authentications when accessing a service or conducting a transaction, and the range of services and transactions that are accessible remotely, online.

Similarly, the use of e-signatures is limited in lower-middle-income and low-income countries for various reasons. E-signatures—when paired with proper regulation—have the same legal standing as traditional signatures, enabling contracts to be signed remotely and facilitating greater
FIGURE 4.4 Gaps in access to official identification, by demographics and country income group, 2021

Sources: Clark, Metz, and Casher 2022; Demirgüç-Kunt et al. 2022.
Note: Information on rural versus urban location was only available for the subset of economies where face-to-face data collection was possible in 2021. Includes respondents ages 15 and older who are over the eligible age for obtaining an ID. HIC = high-income countries; ID = identification; LIC = low-income countries; LMIC = lower-middle-income countries; UMIC = upper-middle-income countries.

trust and assurance in remote transactions, which are essential for a vibrant digital economy. Only 96 economies have fully operationalized both the legal frameworks and the technological infrastructure (for example, public key infrastructure and certificate authorities) for e-signatures. Of these, 42 are high-income countries (of 62 high-income countries) and a further 27 are upper-middle-income countries. An additional 28 economies have both the necessary legal frameworks and the infrastructure but have not yet operationalized them. Some of the key challenges include the limited set of use cases for e-signatures, the cost and complexity of developing sustainable public key infrastructure, and low supervisory capacity to create a competitive marketplace of third-party e-signature providers. For instance, 35 economies have regulations, but are still developing the technological infrastructure.

Enabling seamless exchange and reuse of data, with appropriate safeguards against risks of misuse, is key to improving government services, as well as enabling businesses to reuse responsibly the data that government holds. The “Once Only” principle dictates that people and businesses should only have to provide information to the government on a single occasion and that data can be reused for other transactions. Interoperability frameworks and data exchange platforms (for example, government service buses and API gateways) facilitate data to move both horizontally (such as across ministries) and vertically (across different levels of government). Moreover, when governments can make the data it holds available to people, academia, civil society, and businesses—again, with appropriate safeguards to protect personal data—doing so can unlock innovation. For example, if people can share information about their official driving
history, they may be able to access less expensive and more tailored insurance products. Similarly, if they can share their health information with health care providers, they may receive higher-quality and better-informed care.

Data exchange is an area for improvement: although 89 economies reportedly have a functional data exchange platform, 65 of them are high-income or upper-middle-income countries. Good examples of such data exchange platforms include Singapore’s APEX (Cooper, Marskell, and Chan 2022) and Estonia’s X-Tee, both of which are widely used and depend on consent of the data subject for triggering the exchange of personal data. Estonia has made the underlying technology for X-Tee available as a digital public good (open-source software), which has been used by or has inspired countries such as Cambodia, Finland, Mauritius, and Namibia. A further 24 economies are in the process of building data exchange platforms, leaving 85 economies without this important DPI element. Box 4.4 highlights a few data-sharing examples.

**BOX 4.4 Data-sharing examples: India’s DigiLocker, Singapore’s APEX, and Uganda’s UGHub**

**India’s DigiLocker**

Launched in 2015, DigiLocker is a secure personal document wallet and 1 gigabyte of cloud storage that the government of India offers to every person registered with Aadhaar. Digital documents shared via DigiLocker can be securely verified and have the same legal effect as physical equivalents. Users can either upload scans of documents or request documents to be uploaded on their behalf. Sharing is based on consent of the individual, and users can revoke their consent to third-party access. As of September 2023, there are 197 million users, 6.3 billion issued documents, 1,684 document issuers, and 187 requesters. The COVID-19 pandemic drove significant adoption, with 23 million users in 2019.

**Singapore’s APEX**

APEX is a governmentwide application programming interface (API) management solution (Cooper, Marskell, and Chan 2022) that enables government agencies to publish and manage access to their APIs and to discover other APIs. Unlike the enterprise service bus approach, which creates a central infrastructure that data may pass through, APEX facilitates bilateral connections between systems and databases, which can provide more flexibility and scalability.

The number of APIs supported through APEX has surpassed 2,000, including more than 45 agencies, approximately half of all government agencies in Singapore. The level of traffic has surpassed 100 million transactions per month, with peaks, on average, exceeding 300 million transactions per month. APEX is a backbone of Singapore’s national digital ID (Singpass) and is integrated with the Singpass consented data-sharing service, which empowers Singapore citizens, residents, and businesses to grant access to trusted data that the government holds about them. APEX eases access to services by saving time and lowering costs and improves the quality of data submitted to government agencies and businesses. Singpass is estimated to save as much as S$50 per eKYC transaction conducted for opening a financial account.

**Uganda’s UGHub**

Following the enterprise service bus model of a central infrastructure and using the open-source WSO2 technology stack, UGHub is a systems and data integration platform. As of August 2023 and following two years of operations, 47 public entities and 66 private entities (for example, banks and universities) connected to exchange personal and nonpersonal data in a secure, seamless manner more than 100 million times. UGHub was developed by the National IT Authority, with financing from the World Bank’s Regional Communications Infrastructure Program.
One of the most critical economic development objectives that digital technologies can enable is financial inclusion, which in many low- and middle-income countries has manifested in the form of mobile money accounts and payments. Its aim of “banking the unbanked” has overhauled financial services, especially for individuals in rural areas with no access to formal finance, improving financial inclusion in lower-income countries (Demirgüç-Kunt et al. 2022), and this trend increased during the global pandemic. According to World Bank Findex data collected from around 130 countries, more people had a mobile money account than an account at a financial institution in low-income countries in 2021 (26 percent versus 25 percent; refer to figure 4.5, panel a). Ownership of a mobile money account also grew faster than ownership of an account in a formal financial institution in lower-middle-income and low-income countries from 2017 to 2021.

While the percentage of adults with a formal financial account in low- and middle-income countries jumped to 71 percent in 2021 (from 63 percent in 2017), only 57 percent of adults in low- and middle-income countries made or received some sort of digital payment, and only 37 percent did so with a merchant (Demirgüç-Kunt et al. 2022). In China and Mongolia, more than 80 percent of adults made digital merchant payments in 2021 (refer to figure 4.5, panel b). By contrast, in India, only 12 percent of adults made a digital merchant payment, and two-thirds of those who made a digital merchant payment did so for the first time after the onset of COVID-19. One significant opportunity is the rapid rise of fast or real-time payment systems, which have been launched or announced in about 100 jurisdictions. Together, the 24/7/365 availability of these systems and the instant availability of funds to recipients boost trust and convenience for users, while spurring competition and innovation from a diverse range of providers, including banks and nonbanks.

The COVID-19 crisis highlighted how DPI can play a critical role for governments to deliver social assistance quickly and safely. DPI not only allowed governments to reach an unprecedented number of new beneficiaries, but also allowed them to make payments remotely. Millions of

**FIGURE 4.5 Adoption of digital financial services**

a. Mobile money and financial account ownership, 2017 and 2021

b. Digital merchant payments made, 2021

Source: Demirgüç-Kunt et al. 2022.

Note: HIC = high-income countries; UMIC = upper-middle-income countries; LMIC = lower-middle-income countries; LIC = low-income countries.
people were brought into the social protection and financial system for the first time. Scaling up social assistance presented two separate but related challenges: first, adapting targeting and registration to reach individuals not commonly included in social assistance databases, such as urban informal workers, and second, delivering G2P payments safely and securely in the context of the pandemic.

Countries also used digital systems to tackle the second challenge, with 80 percent of the countries analyzed starting to use digital payments for delivering at least one of their new or expanded social assistance programs as of May 2021 (refer to figure 4.6). Most countries that used digital payments to deliver COVID-response payments had already implemented digital payments to some extent prior to the pandemic; however, several countries used them for the first time, facilitating a long-term shift to modern social assistance payments.

When G2P payments are deposited digitally into accounts—mobile money or traditional accounts, such as banks or microfinance institutions—they not only reach more people quickly and safely and reduce leakages and corruption, but also create a pathway to financial inclusion and women’s economic empowerment. The Global Findex 2021 finds that 865 million account owners (or around 18 percent), including 423 million women in low- and middle-income economies, opened their first financial institution account for the purpose of receiving money from the government. Among those who reported receiving government transfers, around 65 percent received it digitally, with no significant difference between men and women, and around 15 percent did so in cash.

Opening an account and receiving payments into it are just the first step toward financial inclusion. The Global Findex 2021 also shows that in low- and middle-income economies around 7 out of every 10 persons who received government transfers into an account also made a digital payment compared to only about half in 2017. Such payments included using the internet to pay bills or make a purchase (49 percent) or using a mobile account to make an in-store purchase (54 percent). Beyond digital payments, 34 percent also saved in a formal financial institution or through a mobile money account. The increasing use of accounts by beneficiaries for more than taking out cash indicates strong progress toward bridging the gap between access and use of formal financial services.3

Countries that shifted to digital payments during the pandemic, even if partially, now can leverage that investment to facilitate a long-term shift to modern G2P payments. The digitalization of COVID-19 response programs led to an increase in account ownership, and provided a pathway to increasing financial inclusion only if this momentum was leveraged to develop and sustain the necessary enablers. At least 62 countries have leveraged account-based transfers for their COVID-19 response social assistance programs to some extent. Many of them are using accounts as their method of paying social assistance for the first time. Yet in many cases, these account-based payments have been adopted only for temporary COVID-19 programs. Unless governments make conscious efforts to adopt these account-based payments across other social assistance programs and government payment streams, there is a risk of reversing the important strides made in building the ecosystem needed to deliver digital payments.
How to build good DPI

A growing body of experiences, evidence, and principles is cultivating a shared understanding of what is generally needed to make DPI work at scale and what are the risks and challenges (refer to exhibit 4.1). However, what works in a particular country will depend on the local context.

EXHIBIT 4.1 How to build good digital public infrastructure

<table>
<thead>
<tr>
<th>Success factors</th>
<th>Challenges and risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Focus on use cases. Building digital public infrastructure (DPI) for its own sake is unlikely to achieve high adoption. The design of DPI should be driven by solving real-world problems that people, firms, and government agencies face.</td>
<td>Exclusion from services. Poorly designed DPI can create unnecessary barriers for people and firms to access services. Systems and processes need to be reimagined, since digitalizing poor practices will lead to poor digital practices.</td>
</tr>
<tr>
<td>Prioritize inclusion and universal accessibility. DPI should be designed to work for all parts of society, which means accommodating various factors (for example, access to digital infrastructure and devices, awareness, skills, and trust in technology) and ensuring accessibility for individuals with different needs, including those with disabilities.</td>
<td>Data protection and security breaches. Leaks and misuse of data, not just of DPI but also of the applications using DPI, can erode public trust and have potentially disastrous consequences. Continuous investment in security postures and in legal and institutional frameworks for protecting personal data can reduce these risks.</td>
</tr>
<tr>
<td>Build public trust and accountability. Adoption is enabled at a faster rate when all stakeholders have confidence that DPI works as intended and is in their best interests and that grievance redress mechanisms are in place.</td>
<td>Vendor and technology lock-in. Inadequately selected or procured technology can lead to a dependence that makes it harder to adapt DPI and can increase the total cost of ownership in the medium and long terms. The risk can be reduced substantially by building capacity to manage procurement and contracts effectively, by using modular designs, and by adopting open standards.</td>
</tr>
<tr>
<td>A whole-of-country approach and public-private partnership. The shift in mind-set requires coordination and collaboration across a wide range of stakeholders; a whole-of-country approach benefits from having a singular vision.</td>
<td>Inertia and legacy legal frameworks. Resistance to the changes that can be brought about by DPI can come from a variety of sources. A comprehensive review and reform of laws and regulations may be needed to address this key bottleneck.</td>
</tr>
<tr>
<td>Promote interoperability. The true power of DPI comes when different layers or elements can work together to enable exponential innovation. The adoption of common standards and open application programming interfaces can help to address this need.</td>
<td></td>
</tr>
<tr>
<td>Strengthen capacity and culture in government. Civil servants need incentives to take risks and to think and act boldly. Budget and procurement policies may also need to be made fit-for-purpose.</td>
<td></td>
</tr>
<tr>
<td>Cross-border use of DPI. As DPI gains global traction, there is an opportunity for enhanced regional and international cooperation to establish standards for cross-border use. This cooperation includes mutual recognition of digital IDs, interoperable fast payment systems, and secure data sharing. Such cooperation can lower the costs and risks associated with international transactions, such as remittances, access to services across borders, and cross-border data flows.</td>
<td></td>
</tr>
</tbody>
</table>

Notes


2. Such services can be provided through multiple digital identity ecosystems, operated by governments or the private sector, or provided through centralized, federated, or decentralized architectures. In some cases, they are provided by the same entity responsible for traditional forms of official identification (for example, a digital version of a national ID or population register); in others, they are built on top of such systems and leverage them for digital ID onboarding (for example, Europe’s eIDAS federation or new e-wallet or Australia’s Trusted Digital Identity Framework). For a typology of architectures for government-recognized digital identity, refer to World Bank (2022a).

3. This analysis is based on Desai, Klapper, and Natarjan (2022).

References


